VMware envió actualizaciones para abordar dos vulnerabilidades de seguridad en vCenter Server y Cloud Foundation, que podrían ser abusadas por un atacante remoto para obtener acceso a información confidencial.

El más grave de los problemas se refiere a una vulnerabilidad de lectura de archivos arbitraria en vSphere Web Client, rastreado como CVE-2021-21980, este error se calificó con 7.5 de un máximo de 10 en la escala de puntuación CVSS, e impacta en las versiones 6.5 y 6.7 de vCenter Server.

«Un actor malintencionado con acceso de red al puerto 443 en vCenter Server puede explotar este problema para obtener acceso a información confidencial», dijo la compañía en un aviso del 23 de noviembre, acreditando la eliminación del laboratorio de Orz por informar la falla.

La segunda vulnerabilidad corregida por VMware se relaciona con una vulnerabilidad SSRF (Server-Side Request Forgery) en el comportamiento de cliente web de la red de área de almacenamiento virtual (vSAN), que podría permitir que un atacante con acceso de red al puerto 443 en vCenter Server explote la falla accediendo a un servidor interno o una solicitud de URL fuera del servidor.

La compañía otorgó el crédito a magiczero de SGLAB, de Legendsec en Qi'anxin Group por haber descubierto y reportado la vulnerabilidad.

Los ataques SSRF son un tipo de vulnerabilidad de seguridad web que permite a un adversario leer o modificar los recursos internos a los que el servidor de destino tiene acceso mediante el envío de solicitudes HTTP especialmente diseñadas, lo que da como resultado la exposición no autorizada de información.

Los riesgos que surgen de los ataques SSRF son tan graves y generalizados que llegaron a la lista de los 10 principales riesgos de seguridad de aplicaciones web del Open Web Application Security Project (OWASP) para 2021.

Con las soluciones de virtualización de VMware ampliamente utilizadas en las empresas, no sorprende que sus productos se hayan convertido en objetivos lucrativos, para que los actores de amenazas organicen una variedad de ataques contra redes vulnerables.

Para mitigar el riesgo de infiltración, se recomienda que las organizaciones se muevan rápidamente para aplicar las actualizaciones necesarias.